# Unmasking SparkRAT: Detection & macOS Campaign Insights

Published: 2025-01-28 · Archived: 2026-04-05 19:05:35 UTC

SparkRAT, first released on GitHub in 2022 by user XZB-1248, remains a favored tool due to its modular design, web-based user interface, and cross-platform support for Windows, macOS, and Linux systems. The malware has been deployed as a post-exploitation tool in campaigns associated with CVE-2024-27198 and observed in cyber espionage operations targeting government organizations. In our previous post from April last year titled "Spotting SparkRAT: Detection Tactics & Sandbox Findings", we provided a high-level overview of the RAT, analyzing an implant and its C2 server.

In this post, we will:

- Share techniques on detecting SparkRAT servers in the wild.
- Examine a recent sighting: An extension of a suspected DPRK campaign targeting macOS users.

## Understanding SparkRAT Communications and Detection

Developed in Golang, SparkRAT leverages the WebSocket protocol to communicate with the command-and-control server. Following this, the malware moves to HTTP, specifically, a POST request to check for the latest version of the RAT within the repository. By default, the server listens for commands on port **8000**, although this can be easily reconfigured. As we'll demonstrate below, default settings provide a valuable fingerprint for identifying SparkRAT deployments in the wild.

```
GET /ws HTTP/1.1
Host: 67.217.62.106:4443
User-Agent: Go-http-client/1.1
Connection: Upgrade
Key: 4fdab31bb8e2932dfe20f92f3fdea3e6eebd95389486a97ad3543bb1583efe62
Sec-WebSocket-Key: TNBx/zMYLDNEkndzyO0ilg==
Sec-WebSocket-Version: 13
UUID: b43dfc4b543363da522193b18b484cdb
Upgrade: websocket

HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: u2MlXFGMQEqTHxqmBFY9e+PuG+o=
Secret: 1e88ef855eb571f9173bd9487adab8c673b2eb06a72081b5d8ecefa95fcdf6de
```

Figure 1: PCAP screenshot showing SparkRAT initial communications.

For those interested in real-time tracking, our Active C2s page offers scan results for more than 100 tools, both legitimate and malicious, including SparkRAT. This feature, which we are constantly improving, provides detailed visibility into active command-and-control infrastructure.

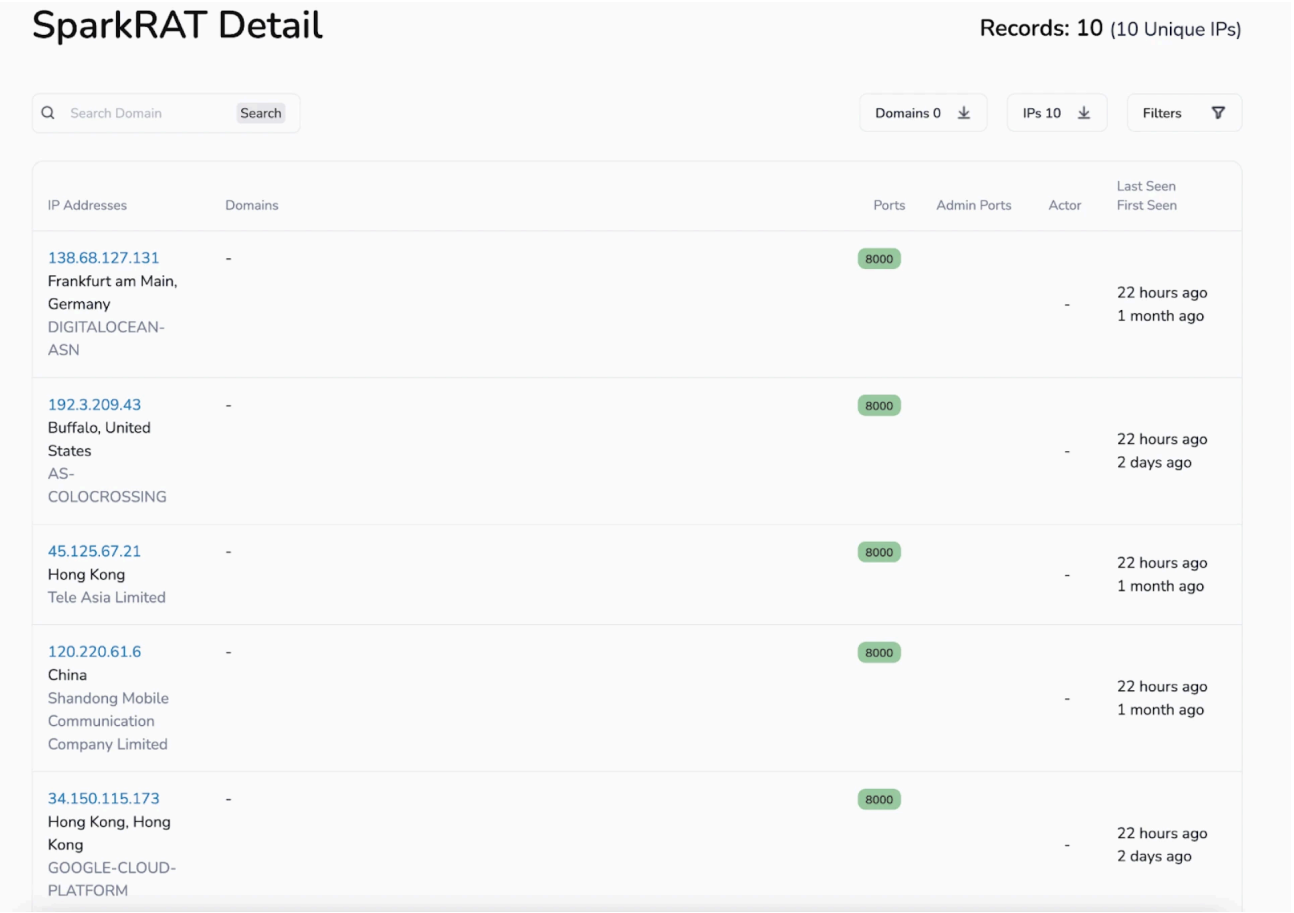


Figure 2: Snippet of the SparkRAT servers we track in Hunt.

## Detection Opportunities

SparkRAT employs HTTP Basic Authentication to restrict access to its C2 server panel, which requires a username/password to be created in the configuration file to proceed. When visiting one of these pages, users will be prompted with a login prompt, which may deter further exploration by casual observers.

When accessing a suspected web panel on the default port 8000, the HTTP response headers include the following:

- HTTP/1.1 401 Unauthorized
- Www-Authenticate: Basic realm=Authorization Required
- -Date
- Content-Length: 0

Notably, standard header fields such as Server, Content-Type, and Connection are omitted, which can serve as additional indicators to filter for potential SparkRAT deployments. As previously discussed, an upgrade check is made via a POST request, as shown in the example below.

```
POST /api/client/update?arch=amd64&commit=08059e95dacafe0bf6e5782f8e2c8ec9cd8c5a17&os=windows HTTP/1.1
Host: 67.217.62.106:4443
User-Agent: SPARK COMMIT: 08059e95dacafe0bf6e5782f8e2c8ec9cd8c5a17
Content-Length: 384
Content-Type: application/octet-stream
Secret: 1e88ef855eb571f9173bd9487adab8c673b2eb06a72081b5d8ecefa95fcdf6de
Accept-Encoding: gzip

.......c.^.^].i..IX./..}..P*.(I.K...........>X.q=....{w...m9..<)..B..7...;E.....y$./.D.K.BA.x.i^.u....S.\.6.~..AN.8..v./...
...,.o..XF.0a.o..........."..kfk6d....N......h@..v.%M...
...r.&}. si
=.\zEO..
t.......jn.h.....h.^0.Y.h.d..]..9?9g....ZS......U.~..V..|]9E...)g{...<......h.#..#P...o.o...G.e   Z......`4Xx
.....:i~s|...|I....z>.>|.-....p...k~...mNn..s=...yg.aM_.........M....y...A.5HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Thu, 24 Oct 2024 19:04:30 GMT
Content-Length: 10

{"code":0}
```

Figure 3: Example request for an upgrade in SparkRAT.

The server expects the following in the path: /api/client/update?arch=*, along with a few other specific headers like the User-Agent with a value of SPARK COMMIT: ", and a similar Secret field. What if we pick a single server to investigate (be a good internet neighbor) and send a POST request to the /api/client/update endpoint?

A suspected SparkRAT server responds with the following:

- HTTP/1.1 400
- Content-Type: application/json; charset=utf-8
- -Date
- Content-Length: 52

More interestingly, the response also includes a response body for further analysis:

```
'{"code":-1,"msg":"${i18n|COMMON.INVALID_PARAMETER}"}'
```

Copy

We use some additional tricks to validate SparkRAT servers. However, combining the first response headers on port 8000 and then looking for the above JSON response should be a great starting point for those looking for C2s to investigate/research.

## Suspected DPRK Campaign Persists with SparkRAT Activity

In late November 2024, researcher Germán Fernández (@1ZRR4H) highlighted a possible campaign delivering SparkRAT via fake meeting pages and domains, initially identified by @malwareHunterTeam. Around the same time,

Chris Duggan, @TLP_R3D, shared additional insights, including a search query and a list of IP addresses likely associated with the activity.

Using Hunt to actively scan for RAT servers, we investigated further to identify any infrastructure that had not yet been publicly reported. Somewhat unexpectedly, our scans revealed three additional servers, each hosting open directories containing SparkRAT implants and exhibiting tactics consistent with those previously described.

The identified IPs, along with their ASNs, locations, and associated domains, are as follows:

| IP Address | ASN | Location | Domain(s) |
|---|---|---|---|
| 152.32.138[.]108 | UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED | KR | gsoonmann[.]site<br>gmnormails[.]site<br>gmoonsom[.]site<br>nasanecesoi[.]site<br>gmoocsoom[.]site<br>gmcomamz[.]site<br>namerowem[.]site<br>gmoosomnoem[.]site<br>mncomgom[.]site<br>ggnmcomas[.]site |
| 15.235.130[.]160 | OVH SAS | SG | remote.henh247[.]net<br>updatetiker[.]net |
| 118.194.249[.]38 | UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED | KR | gomncomow[.]site<br>gooczmmnc[.]site<br>gnmoommle[.]space |

These findings indicate that this campaign is still going strong, albeit with some differences in delivery tactics. Unlike the previously reported activity, we observed no meeting-related domains or web pages. Additionally, at least one of the open directories used a different path to deliver SparkRAT than previously documented. We will examine the files and open directories uncovered in this activity in the sections below.

### 152.32.138[.]108

Hosted in Seoul, South Korea, this server exhibits several characteristics frequently associated with DPRK-linked infrastructure. These include the UCLOUD ASN, an Apache HTTPD server stack, top-level domains (TLDs) like .site, .space, and others registered under Namecheap, and Let's Encrypt TLS certificates.

An exposed directory located at /dev on port 443 contains three files and two empty subfolders. Among the files are two bash scripts (dev.sh and test.sh), which perform identical actions. Of note, the directory path aligns with the download URL mentioned in the X/Twitter post, which used `/dev/ticker`. The final file is client.bin, which is a SparkRAT client.

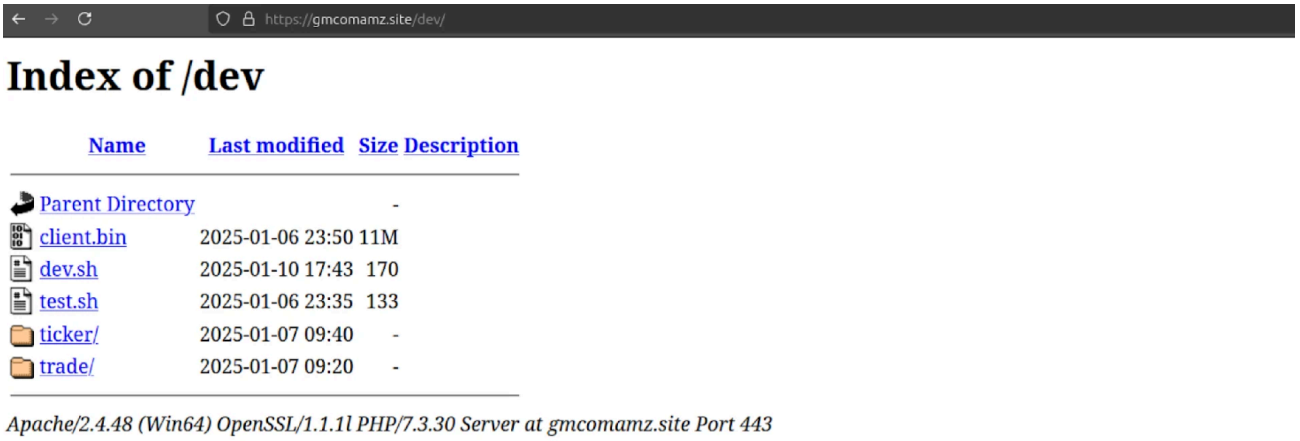


Figure 4: Screenshot of the open directory at https://gmcomamz[.]site:443.

Both scripts use `curl` to download client.bin from the URL `http://updatetiker[.]site/dev/client.bin`, hosted at the following IP to be discussed: 15.235.130[.]160. The file is saved to `/Users/shared/pull.bin` using the `-o` flag to specify the output file name and the `-L` flag to follow redirects. Once downloaded, `chmod 777` sets full read, write, and execute permissions to pull.bin for all users. Finally, the renamed file is executed as a background process.

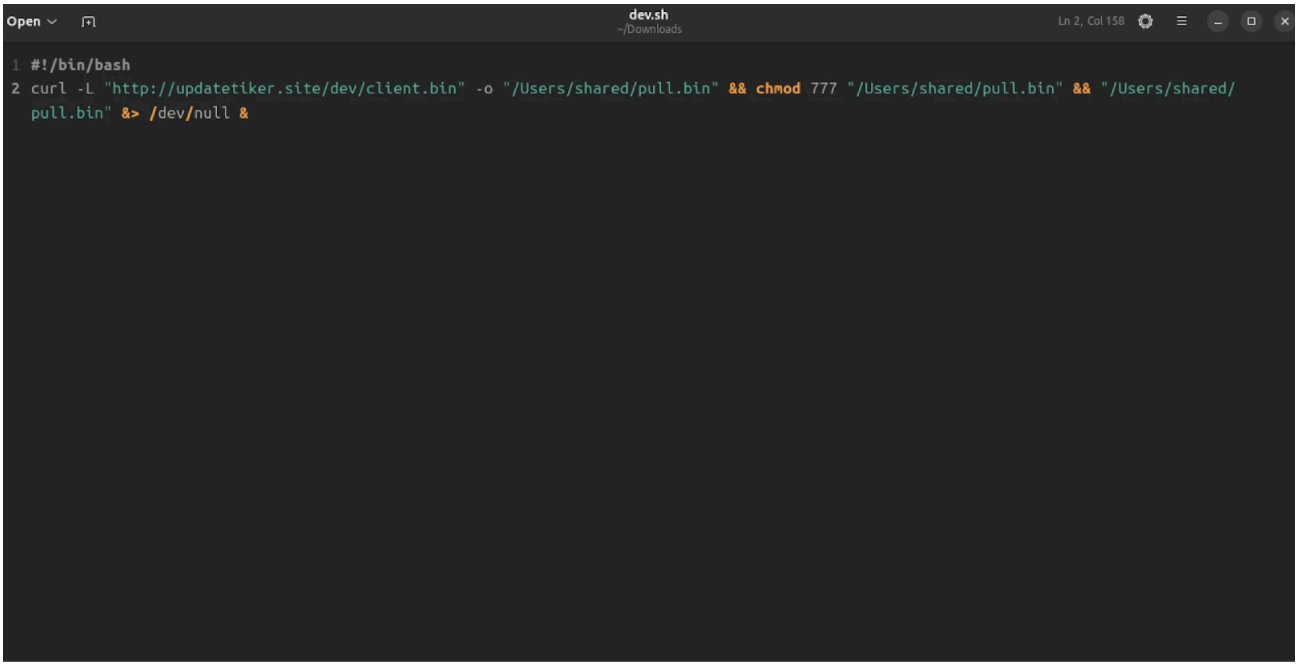


Figure 5: Commands in the dev.sh file.

### File Analysis: client.bin

The file `client.bin` (SHA-256: cd313c9b706c2ba9f50d338305c456ad3392572efe387a83093b09d2cb6f1b56) is a 64-bit Mach-O binary containing numerous strings from the SparkRAT repository and detected as malicious by 16 of

63 vendors. Upon execution, the malware creates and drops the file com.second.startup.plist in /Users/run, configuring it to execute every 10 minutes as part of its persistence mechanism.

The malware attempts multiple TCP connections to 51.79.218[.]159:8000, an OVH SAS server located in Singapore. Although the port was unresponsive during our research, port 80 hosts a webpage claiming to be an online gaming platform, One68, aimed at Vietnamese speakers. The page's title, "one68.top - Game Bai Dinh Cao," translates to "High-Class Card Game." As shown in the figure below, the site features a download button for an Android APK file (one68_1_1.0.apk, SHA-256: ffe4cfde23a1ef557f7dc56f53b3713d8faa9e47ae6562b61ffa1887e5d2d56e).

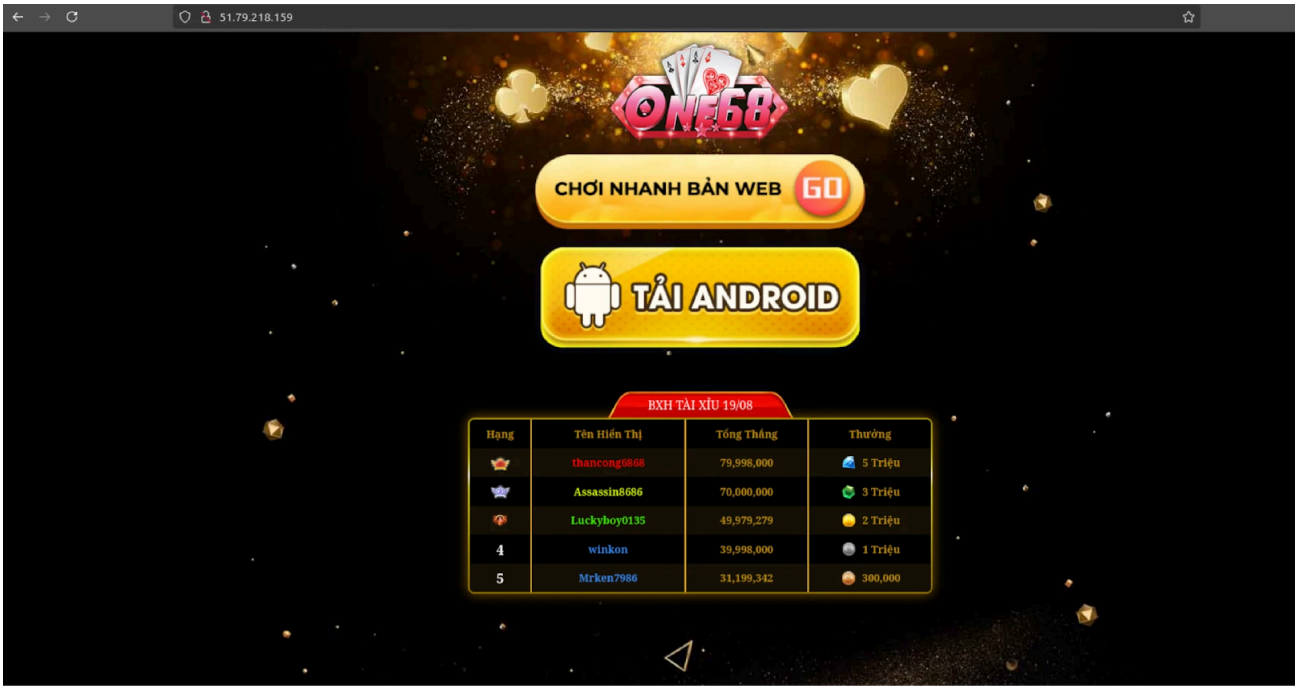


Figure 6: Online gaming webpage hosted on port 80 of 51.79.218[.]159.

While our initial analysis confirms specific capabilities of the malware, such as its networking behavior, we were unable to extract a broader range of its functionalities. Further investigation into the binary is ongoing.

The APK makes a GET request to `http://one68[.]top/client`, and the server responds with HTTP 101 Switching Protocols indicating an upgrade to a WebSocket connection. Notably, the response includes CloudFlare-specific headers indicating the service is used to hinder analysis and hide the above IP address.

```
GET https://one68.top/client

Remote address:
104.21.12.146:443

Request
GET /client HTTP/1.1
Host: one68.top
Connection: Upgrade
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Linux; Android 13; sdk_gphone_x86_64 Build/TE1A.220922.033; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/103.0.5060.71 Mobile
Safari/537.36
Upgrade: websocket
Origin: https://one68.top
Sec-WebSocket-Version: 13
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Sec-WebSocket-Key: DAxSciMpN1IcHkwC2MX6lQ==
Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits

Response
HTTP/1.1 101 Switching Protocols
Date: Sun, 26 Jan 2025 14:16:54 GMT
Connection: upgrade
Upgrade: websocket
Sec-WebSocket-Accept: WYRp2gSWI1CMUtsxXJWPXI2dnXM=
cf-cache-status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=Y2h%2B0BvlCjXOd2xzA%2BK54BqosShHNwLF9czrRUHtDB0C9Y39ixZiY0gchXD%2FzXVDB1km8MgMHHgx5eSoRk3KlRS9mFi0hWk%2FLxQuvGpGF3btl0BRy%2FvllaXJHuw%3D"}],"group":"cf-
nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 90811f981b8ef23a-LHR
alt-svc: h3=":443"; ma=86400
server-timing: cfL4;desc="?
proto=TCP&rtt=39482&min_rtt=39475&rtt_var=14818&sent=3&recv=6&lost=0&retrans=0&sent_bytes=218&recv_bytes=1175&delivery_rate=34020&cwnd=250&unsent_bytes=0&cid=6e762725e88a8321
&ts=423&x=0"
```

Figure 7: Screenshot of the APK GET request to the /client endpoint (Triage).

### 15.235.130.160

Our scans identified 15.235.130.160 as an active SparkRAT C2 server operating on the default port 8000 approximately two weeks ago. Alongside the download domain updatetiker[.]site, the server also hosts additional domains, including `henho247[.]net` and `remote.henho247[.]net`.

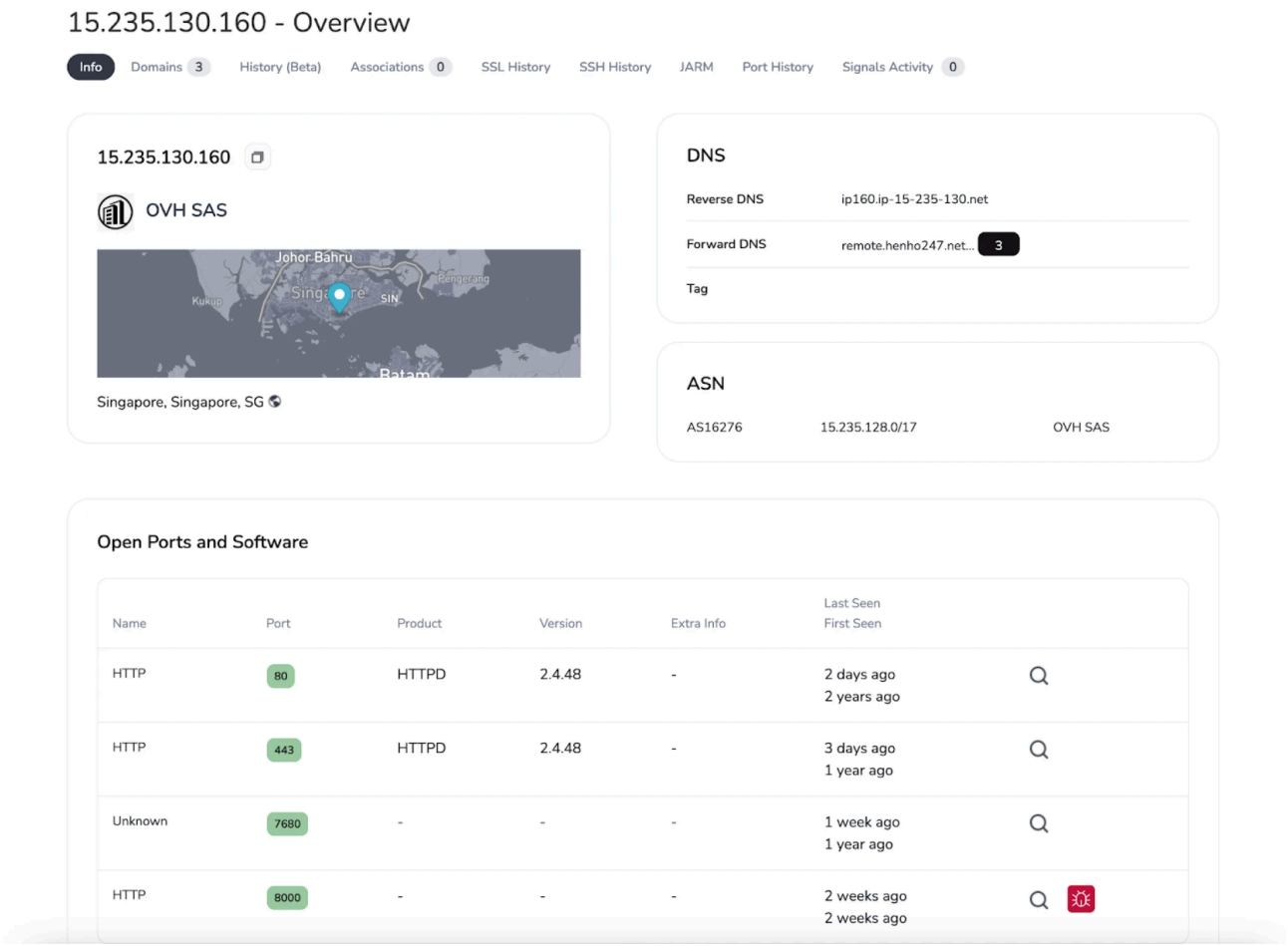


Figure 8: Screenshot of the IP overview and the detected SparkRAT C2 on port 8000 (Hunt).

An open directory on this server contains files with names consistent with those observed on the previously discussed server, such as client.bin and dev.sh, but the empty subfolders are uniquely labeled `/tradem/` and `/tradew/`. The client.bin file on this system was last modified on January 10, four days later than the version hosted on the earlier server.

The binary (SHA-256: 52277d43d2f5e8fa8c856e1c098a1ff260a956f0598e16c8fb1b38e3a9374d15) executes similarly to the earlier sample but establishes communication with the same C2 on port 8000.

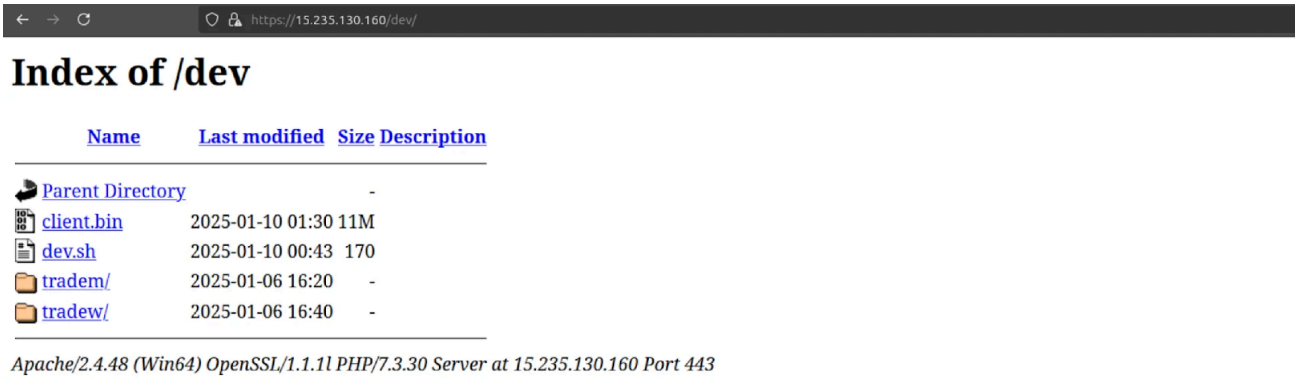


Figure 9: Open directory for 15.32.138.108.

### 118.194.249[.]38

While operational security appears to have been more carefully considered on this server, as no open directories were identified, the final IP in our analysis resolves to three domains that align with previously observed patterns:

- gomncomow[.]site
- gooczmmnc[.]site
- gnmoommle[.]space

We'll continue to monitor this IP as activity has been observed on multiple ports over the past two days. Although the absence of an open directory limits immediate analysis, its domain patterns and recent behavior suggest it remains part of the threat actors' infrastructure.

## Conclusion

SparkRAT remains a persistent threat due to its adaptability and consistent use by adversaries across platforms. The findings in this blog highlight how a detailed analysis of its infrastructure and associated artifacts can uncover additional activity, offering defenders valuable opportunities to monitor and disrupt these operations proactively.

The suspicious APK and its connection to a webpage mimicking a Vietnamese online gaming platform underscore the evolving tactics threat actors employ to target unsuspecting users. These techniques, coupled with SparkRAT's modular design and cross-platform capabilities, make it a versatile tool for adversaries seeking to achieve persistence, exfiltration, and other malicious objectives.

Our research team will continue to refine our detection methods and expand our scanning beyond the default port, which will allow us to uncover additional SparkRAT infrastructure, ensuring the security community is equipped with actionable intelligence to combat this threat.

## Network Observables and Indicators of Compromise (IOCs)

| IP Address | Hosting Provider | Location |
|---|---|---|
| 152.32.138[.]108 | UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED | KR |
| 15.235.130[.]160 | OVH SAS | SG |
| 118.194.249[.]38 | UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED | KR |
| 51.79.218[.]159 | OVH SAS | SG |

## Host Observables and Indicators of Compromise

| Filename | SHA-256 Hash | Notes |
|---|---|---|
| client.bin | cd313c9b706c2ba9f50d338305c456ad3392572efe387a83093b09d2cb6f1b56 | Hosted on an open directory at 152.32.138[.]108 |
| client.bin | 52277d43d2f5e8fa8c856e1c098a1ff260a956f0598e16c8fb1b38e3a9374d15 | Found on an exposed directory at 15.235.130[.]160 |
| one68_1_1.0.apk | ffe4cfde23a1ef557f7dc56f53b3713d8faa9e47ae6562b61ffa1887e5d2d56e | Downloadable file on one68[.]top |

---

Source: https://hunt.io/blog/sparkrat-server-detection-macos-activity-and-malicious-connections